PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of: Menno Anne Treffers et al.	
US Application No. 09/930,654	Examiner: Popham, Jeffery D.
Confirmation No. 1920	
Filed: August 15, 2001	Group Art Unit: 2137
Attorney Docket No. 93418.000047	

For: METHOD AND DEVICE FOR CONTROLLING DISTRIBUTION AND USE OF DIGITAL WORKS

July 21, 2008 (Monday)

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANTS' REQUEST FOR REHEARING

Appellants request a rehearing of the Board's decision of May 19, 2008, in the subject application, because it is believed that the Board considered a wrong version of independent claim 1 and therefore misapprehended both the claim and the teaching of the cited patent documents.

The claim set forth on page 1 of the Decision on Appeal is not an accurate copy of claim 1 on appeal. The actual text of claim 1 as appealed is contained in the Appendix to the Appeal Brief. The claim considered by the Board appears to be the claim originally filed, not including the amendments made in the Amendment certified as being mailed on August 15, 2005. Favorable reconsideration of this Appeal is requested, because it is believed that the Board misapprehended the scope of independent claim 1.

Appellants also submit that the Board misapprehended the teachings of the cited patent documents, and the applicability of those claims to the pending claims.

The present invention requires, in independent claim 1, changing a hidden information stored in a hidden channel and used for encrypting or verifying said usage right information when said usage right information has changed.

Similarly, independent claim 11, which relates to a record carrier for storing a digital work and a usage right information, features that the record carrier includes a hidden channel not accessible by commercial reproducing devices, hidden information stored in the hidden channel, and the hidden information being used for encrypting or verifying the usage right information and being changed when the usage right information has changed.

Also, independent claim 13, which relates to a device for controlling distribution and use of a digital work, features an updating means for updating attached usage right information with every use of a digital work. The updating means also changes hidden information stored in a hidden channel and used for encrypting or verifying the usage right information when the usage right information has changed.

Accordingly, in each of the independent claims, hidden information used for encrypting or verifying usage right information is stored in a hidden channel ***on the media*** and is updated when the usage right information has changed.

Before undertaking a detailed technical discussion of the cited documents and their application to the claims, a review of the invention is worthwhile. The present invention is particularly directed to overcoming a type of unauthorized copying referred to as a "replay attack." In a standard replay attack, content and associated usage rights contained on a disc are copied onto another memory, e.g., a disc drive. The copy cannot be played when contained on the disc drive, because the content and/or usage rights are conventionally encrypted using a key that is unique to the disc. However, when the usage right is exhausted, the copy stored on the disc drive can be re-copied to the disc, refreshig the usage conditions and thus allowing the user to make and play unauthorized uses of the digital work.

Generally speaking, the present invention thwarts such a replay attack by hiding information used for encrypting or verifying usage right information in a hidden channel that cannot be copied onto a memory on a record carrier (the physical media, such as a DVD) and by changing the hidden information on the DVD hidden channel when the usage right information has changed. More particularly, copying the digital work and associated usage right information onto another memory will not copy the hidden information. And, each time the usage right information is changed, e.g., each time the original digital work is played, the hidden information for encrypting or verifying the usage right information is changed. Thus, in the event that a pirate re-copies the original digital work and usage right conditions onto the record carrier, the hidden information, by virtue of being changed from its original state on the media (DVD), would not correspond to the original characteristics of the usage right information. The digital work re-copied to the disc could not be played.

The documents relied upon by the Examiner deal in varying degrees with encryption of information and/or keys. However, the unique combinations claimed by Appellants for overcoming a replay attack are not taught by, nor are they obvious from, those documents. The encryption techniques of the cited documents could be circumvented using the same replay attack that Appellants have devised a unique way to overcome or by other known techniques. Specifically, the cited documents do not teach changing the hidden information on the record carrier and thus could not function in the unique manner contemplated by Appellants.

In one embodiment described in the application, the usage right information is a number of times that a digital work can be played. Each time the digital work is played, the number of times left to be played decreases (i.e., is changed), until the user's rights are exhausted. Also according to this embodiment, the usage right information is encrypted with a key, and that key is hidden. When the usage right information changes, i.e., in this embodiment the number of plays decreases, the hidden key also is changed. Thus, and as set forth in the claim, the hidden information (a hidden key) changes when usage right information (number of times for use) has changed. The invention is particularly useful because a would-be pirate of the digital work would not be able to obtain the hidden key upon creating an illegal copy of the disk, and a bit-for-bit copy of the work would thus not be playable.

The Examiner has taken the position that independent claims 1, 11, and 13 are obvious over the combination of *Shear et al.*, *Downs et al.*, and *Ginter et al.* Appellants disagree and request a rehearing because it is believed that the board misapprehended the teachings of the three cited documents.

Shear et al. teaches a disk 100 as a storage media that stores metadata 202 and content (or properties) 200. The disk also stores an encrypted key block 208 and one or more hidden keys. As described in paragraphs [0216] – [0218], the key block 208 provides cryptographic keys for use in decrypting one or more properties 200 and/or one or more metadata blocks 202. In the embodiment shown in Figure 3, the disk 100 stores decryption keys for decrypting key block 208 on the medium as the hidden keys 210. At paragraph [0080], *Shear et al.* notes "the storage medium itself carries key block decryption key(s) in a hidden portion of the storage medium not normally accessible through typical access and/or copying techniques. This hidden key may be used by a drive to decrypt the encrypted key block--such decrypted key block then being used to selectively decrypt content and related information carried by the medium." Thus, *Shear et al.* teaches hidden keys for decrypting a key block containing keys used to decrypt content.

In paragraph [220], *Shear et al.* also discloses that "the keys [namely, the key block 208] required to decrypt protected content 200, 202 [may be] provided within [a] secure container 206." In addition to containing the key block, *Shear et al.* discloses that the secure container also can include a control set 204, which can include a permissions record 306. According to *Shear et al.*, the secure container is cryptographically protected, but *Shear et al.* provides limited guidance as to what constitutes this cryptographic protection. In the background of the invention section, *Shear et al.* notes that a secure container could be a DigiBox, which is known in the art. A DigiBox is not understood to be accessed by hidden keys on a record carrier and there has been now showing that this is the case. Moreover, there has been no showing as to why it would have been obvious to use hidden keys to access the described secure container.

Thus, *Shear et al.* fails to teach or suggest either of (1) hidden information on a record carrier that is used for encrypting or verifying usage right information and (2) changing such

hidden information when the usage right information is changed. That publication teaches only hidden keys stored on a disk that are used to decrypt key blocks containing keys for decrypting content and that the key blocks may be contained in secure containers.

According to the Examiner, *Downs et al.* teaches updating attached usage right information with every use of a digital work. *Downs et al.* teaches that content usage conditions are stored in an end-user device, e.g., a computer or the like. As described in column 21, lines 51-60, "[t]he Player Application 195 generates a scrambling key for each Content item, and the key is encrypted and hidden in the End-User Device(s) 109. Then, every time the End-User Device(s) 109 accesses the Content 113 for copy or play, the End-User Device(s) 109 verifies the copy/play code before allowing the de-scrambling of the Content 113 and the execution of the play or copy. The End-User Device(s) 109 also appropriately updates the copy/play code in the original copy of the Content 113 and on any new secondary copy." Even conceding that *Downs et al.* teaches updating attached usage right information with every use of a digital work, *Downs et al.* still fails to teach either of (1) hidden information on a record carrier that is used for encrypting or verifying usage right information (the hidden keys of *Downs et al.* are for decrypting content and are stored on the end-user device) and (2) changing the hidden information when the usage right information is changed (*Downs et al.* only teaches updating usage right information).

Ginter et al. also does not teach these features. The Examiner relies on column 136, lines 37-42 of that patent, which teaches that "[i]n the preferred embodiment, the one or more keys used to encrypt each permission record 808 or other management information record will be changed every time the record is updated (or after a certain one or more events). In this event, the updated record is re-encrypted with new one or more keys." *Ginter et al.* also discloses, at column 136, lines 28-31, that "permission records 808 and key blocks 810 for each property can be encrypted with a private DES key that is stored only in the secure memory of an SPU 500.... Alternatively, the key blocks 810 can be encrypted with the end user's public key, making those key blocks usable only to the SPU 500 that stores the corresponding private key (or other secure, encryption/security techniques can be employed." Thus, *Ginter et al.* is understood to teach changing keys used to encrypt permission records when a permission record is updated.

However, those keys are not hidden on a record carrier; they are on the secure memory of a Secure Processing Unit. Thus, *Ginter et al.* also fails to teach (1) hidden information on a record carrier that is used for encrypting or verifying usage right information (the hidden keys are for decrypting content and are stored on the end-user device) and (2) changing the hidden information when the usage right information is changed.

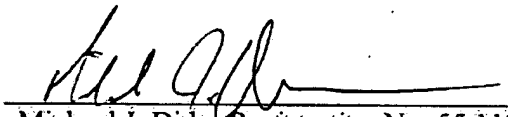
Ginter et al. is assigned to the same assignee as *Shear et al.* and also discusses in some detail the secure container concept presented in *Shear et al.* In fact, the Board of Appeals notes that Figure 3A of *Shear et al.* is substantially the same as Figure 5B of *Ginter et al.*, and both of those figures show a secure container. According to the disclosure of *Ginter et al.*, the secure container is understood to be a means by which data can be sent between users in a secure manner. *Ginter et al.* also does not teach that the secure container is opened by keys hidden on a record carrier.

The features described above, and asserted to not be shown by the three cited documents also are not obvious from a proper combination of these documents. Appellants submit that to one of ordinary skill in the art, the combination of *Shear et al.*, *Downs et al.*, and *Ginter et al.* at best would teach a storage container on a record carrier, with the storage container storing an encrypted key block (having keys for decrypting content) and usage right information. The keys for decrypting the storage container are stored on the user's device, not the record carrier, and may be encrypted using a private DES key. When content on the record carrier is to be played, the keys on the user's device decrypt the storage container to access the encrypted key block and the permission rights. Hidden keys on the record carrier then may be used to decrypt the key block, and the permission rights may be updated. According to *Ginter et al.*, the keys in the device, i.e., for decrypting the storage container, may be changed when the content is viewed.

This combined teaching is distinct from that of the claimed invention, in which the hidden information, which is on the record carrier and used for encrypting or verifying usage right information, is changed each time the usage right information has changed.

For the foregoing reasons, Appellants submit that the combination of *Shear et al.*, *Downs et al.*, and *Ginter et al.*, fails to teach or render obvious the subject matter of independent claims 1, 11, and 13. Favorable reconsideration on rehearing respectfully is requested.

Respectfully submitted,



Michael J. Didas Registration No. 55,112
Customer Number 23387
HARTER, SECREST & EMERY LLP
1600 Bausch & Lomb Place
Rochester, New York 14604
Telephone: 585-231-1411
Fax: 585-232-2152